NOUVELLES ANNALES DE MATHÉMATIQUES

G. H. NIEVENGLOSKI

Note sur la limite supérieure du nombre de divisions à faire pour trouver le plus grand commun diviseur de deux nombres

Nouvelles annales de mathématiques 1re série, tome 4 (1845), p. 568-573

<http://www.numdam.org/item?id=NAM_1845_1_4__568_0>

NOTE

Sur la limite supérieure du nombre de divisions à faire pour trouver le plus grand commun diviseur de deux nombres.

PAR M. G. H. NIEVENGLOSKI,
Répétiteur au Collége royal de Saint-Louis.

—

I.

Soient A et B deux nombres dont on cherche le plus grand commun diviseur. On sait qu'aucun reste, sauf le dernier, ne peut être égal à la moitié du diviseur respectif ; car si cela avait lieu pour un reste quelconque, il serait le plus grand commun diviseur, et par conséquent il devrait être le dernier, ce qui n'est pas ; d'après cela, appelons R_1, R_2, R_3, .. R_n les restes successifs, mais chacun plus petit que la moitié du diviseur respectif, en forçant bien entendu les quotients s'il le faut, comme on le fait ordinairement pour abréger les calculs.

On aura :

$$R_1 < \frac{B}{2}$$

$$R_2 < \frac{R_1}{2}$$

. . . . . .

. . . . . .

$$R_n < \frac{R_{n-1}}{2}$$

d'où en multipliant membre à membre

$$R^n < \frac{B}{2^n}.$$

Il est clair que le nombre des divisions indiqué par celui des restes, sera le plus grand possible, lorsque A et B sont premiers entre eux ;

alors $$R_n = 1. \text{ et } 2^n < B.$$

Il s'agit de savoir quelle est la plus grande valeur entière de n.

Or, si chaque reste était égal à la moitié du diviseur respectif, on aurait :

$$2^n = B \text{ d'où } n = \frac{\log B}{\log 2}.$$

En appelant k le nombre des chiffres de B, comme

$$\log B < k, \log 2 > 0,3,$$

il viendrait :

$$n < \frac{10k}{3};$$

et n devant être entier quel que soit k, on aurait :

$$n \leqq 3k;$$

c'est-à-dire, qu'en supposant chaque reste égal à la moitié du diviseur respectif, n serait tout au plus égal à $3k$; mais ces restes, sauf le dernier, sont tous plus petits que la moitié des diviseurs, donc $n < 3k$.

Il résulte de là que le nombre des divisions pour trouver le plus grand commun diviseur de deux nombres est *toujours moindre que le triple des chiffres* du plus petit nombre.

Prenons pour exemple 196 et 75. Comme le plus petit nombre a deux chiffres, le nombre de divisions pour trouver le plus grand diviseur commun est moindre que 3×2 ; en effet, on trouve pour restes : 29, 12, 5, 2, 1 ; ce qui indique bien *cinq* divisions (*).

(*) Voir tome IV, p. 71. Tm.

II.

Sur la détermination du reste lorsqu'on a trouvé par la division la seconde partie d'une racine carrée.

Soit N un nombre, a la partie trouvée contenant $k+1$ chiffres de sa racine carrée. On sait comment se trouvent par une simple division les k chiffres suivants de cette racine ; mais pour être plus clair dans la suite, je demande la permission de reprendre les raisonnements qui conduisent à cette opération.

Soit b la partie inconnue de la racine cherchée, on a :

$$N = a^2 + 2ab + b^2, \text{ d'où } \frac{N - a^2}{2a} = b + \frac{b^2}{2a},$$

ou bien, en appelant q le quotient entier et r le reste de la division de $N - a^2$,

$$q + \frac{r}{2a} = b + \frac{b^2}{2a} \qquad (1)$$

On a évidemment $r < 2a$, $b^2 < a$; car la valeur relative de a contient $2k+1$ chiffres, tandis que b^2 en renferme au plus $2k$; donc si $b < q$ la différence

$$b - q = \frac{r - b^2}{2a} < 1 ;$$

si au contraire $b > q$ la différence

$$q - b = \frac{1}{2} \cdot \frac{b^2 - r}{a} < \frac{1}{2}.$$

Il suit de là, qu'en prenant le quotient entier q pour la partie cherchée b, $a+q$ sera la racine carrée extraite à moins *de* 1 *près si c'est par défaut*, et à moins *de* 1/2 *près si c'est par excès.*

Or l'égalité (1) montre que, si $b = q$, on a $r = b^2 = q^2$; si $b > q$ on a $r > b^2$ et à plus forte raison $r > q^2$; enfin

$b < q$ donne $r < b^2$, et à plus forte raison $r < q^2$: donc réciproquement 1° si $r = q^2$ on a $b = q$, alors $a + q$ est la racine carrée parfaite ; 2° si $r > q^2$ on a $b > q$, et $a + q$ est la racine carrée extraite par *défaut* à *moins d'une unité près*. Enfin 3° si $r > q^2$ on a $b > q$, et partant $a + q$ est la racine carrée extraite par *excès* à *moins d'une demi-unité près*.

Ayant ainsi trouvé par la division les k derniers chiffres de la racine carrée approchée, il s'agit de déterminer le véritable reste R, je veux dire la différence entre le nombre N et le carré de sa racine $a+q$ par défaut, sans effectuer ce carré ni même former de double produit. Voici comment :

1° Lorsque la racine est extraite par défaut, si l'on appelle ε l'erreur que l'on commet en prenant q pour b, on aura $b = q + \varepsilon$, et par conséquent le reste

$$R = (a + q + \varepsilon)^2 - (a + q)^2 = 2(a + q)\varepsilon + \varepsilon^2 ;$$

d'ailleurs la substitution de $q + \varepsilon$ pour b dans l'égalité (1) donne, toute réduction faite, $2(a+q)\varepsilon + \varepsilon^2 = r - q^2$; donc le reste $R = r - q^2$.

2° Lorsque la racine est extraite par excès, la différence $q^2 - r$ indique ce qui manque au nombre N pour être carré parfait ; en effet on a alors, $q = b - \varepsilon$, et le manque $(a+q)^2 - N = (a+q)^2 - (a+q-\varepsilon)^2 = 2(a+q)\varepsilon - \varepsilon^2$; d'une autre part, en remplaçant b par $q - \varepsilon$ dans l'égalité (1), il vient $2(a+q)\varepsilon - \varepsilon^2 = q^2 - r$; donc le manque $(a+q)^2 - N = q^2 - r$. Il est aisé de voir par là qu'on obtiendra le reste R en retranchant le manque $q^2 - r$ augmenté de 1 du double de la racine trouvée, savoir :

$$R = 2(a+q) - (q^2 - r + 1).$$

Il n'y a dans cette détermination de R qu'un seul calcul pénible, c'est celui de q^2.

Les deux exemples suivants achèveront l'explication.

I. Soit à extraire la racine carrée de 199996164

$$\sqrt{199996164} = 141$$

99 24
399 281
118

Ayant obtenu trois chiffres, on peut calculer les deux suivants par une simple division que voici.....

11861 64 | 282 00
581 42
1764

On a ici $N - a^2 = 1186164$, $2a = 28200$, et l'on trouve

$$q = 42,\ r = 1764.\ \text{Or}\ q^2 = 1764,$$

donc $r = q^2$ et par conséquent 14142 est la racine carrée parfaite.

II. Extraire la racine carrée de 3.

On aura d'abord

$$\sqrt{3} = 1{,}732 \text{ et } R = 176.$$

On trouvera maintenant les trois chiffres suivants par la division ci-contre.....

176000 | 3464
2800 050

On a ainsi : $q = 050$. $r = 2800000$; et comme $q^2 = 2500$ la racine est extraite par défaut ; par suite

$$R = r - q^2 = 2797500, \text{ et } \sqrt{3} = 1{,}732050.$$

En continuant, on déterminera les 6 chiffres suivants par la division ci-contre.....

27975000000 00 | 34641 00
262200 807569
197130
239250
314040
2271

On obtient $q = 807569$ et $r = 227100000000$; il est facile de voir ici que $r < q^2$; en conséquence

$$\sqrt{3} = 1,732050807596$$

est extraite par excès à moins de 1/2 près.

Pour déterminer le reste R , on a d'abord

$$q^2 = 652167689761$$

et ensuite le manque $q^2 - r = 425067689761$; par conséquent

$$R = 2(a+q) - (q^2 - r + 1) = 2039033925376.$$

On peut maintenant trouver les 12 chiffres suivants, etc... Si l'on veut vérifier la racine trouvée en employant la preuve par 11, on n'a pas besoin de calculer R , ni $q^2 - r$; il suffit de connaître q et r. L'explication en serait superflue.